

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/SG05/000037

International filing date: 14 February 2005 (14.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: IN
Number: 336/CHE/2004
Filing date: 15 June 2004 (15.06.2004)

Date of receipt at the International Bureau: 13 May 2005 (13.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse



INTELLECTUAL PROPERTY
INDIA



**GOVERNMENT OF INDIA
PATENT OFFICE**

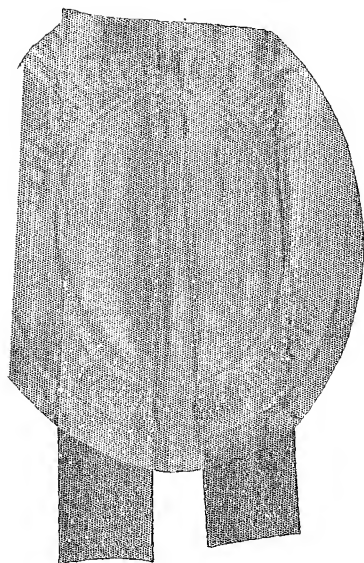
**Ministry of Commerce and Industry
Department of Industrial Policy and Promotion**

It is hereby certified that annexed here to is a true copy of **Application, Provisional Specification & Drawings** of the patent application as filed and detailed below:-

Date of application : 15-06-2004

Application No : 336/CHE/2004

Applicants : M/s. Matrix View Technologies (India) Private Limited,
No. 69, Mahalakshmi Koil Street, Kalakshetra Colony,
Besant Nagar, Chennai – 600 090. India an Indian
Company



In witness there of
I have here unto set my hand

Dated this the 01st day of April 2005
11th day of Chaitra, 1926(Saka)

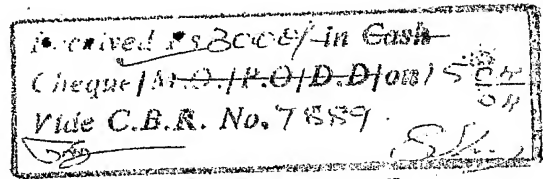
By Authority of
**THE CONTROLLER GENERAL OF PATENTS,
DESIGNS AND TRADE MARKS.**


(M.S.VENKATARAMAN)

ASSISTANT CONTROLLER OF PATENTS & DESIGNS



PATENT OFFICE BRANCH
Guna Complex, 6th Floor, Annex.II
No.443, Anna Salai, Teynampet,
Chennai – 600 018. India.



FORM 1

THE PATENTS ACT, 1970
(39 OF 1970)

APPLICATION FOR GRANT OF A PATENT
(SEE SECTIONS 5(2), 7, 54 AND 135 AND RULE 39)

1. WE, MATRIXVIEW TECHNOLOGIES (INDIA) PRIVATE LIMITED,
of NO. 69, MAHALAKSHMI KOIL STREET,
KALAKSHETRA COLONY, BESANT NAGAR, CHENNAI -600090,
INDIA
AN INDIAN COMPANY

2. hereby declare -

- (a) that we are in possession of an invention titled
"REPETITION CODED COMPRESSION FOR ENCRYPTING HIGHLY
CORRELATED DATA "
- (b) that the Provisional Specification relating to this invention is filed with this
application.
- (c) that there is no lawful ground of objection to the grant of a Patent to us.

3. We further declare that the inventors for the said invention is/are :

NAME (a)	ADDRESS (b)	NATIONALITY (c)
THIAGARAJAN ARVIND	H24/6, VAIGAI STREET, BESANT NAGAR, 600090 CHENNAI, TAMIL NADU, INDIA	INDIAN

4. That we are assignees of the inventor.

5. That our address for service in India is as follows:- D. P. AHUJA & CO., 53 Syed
Amir Ali Avenue, Calcutta 700 019, West Bengal, India. TEL: (033)22819195,
FAX: (033)24757524.

6. That to the best of our knowledge, information and belief the fact and matters
stated herein are correct and that there is no lawful ground of objection to the grant
of patent to us on this application.

7. Following are the attachments with the application:

- (a) Provisional Specification (2 copies)
(b) Statement and Undertaking on Form 3 in duplicate
(c) Formal drawings (12 sheets) (Provisional) in duplicate
(d) Rs 3,000/- by cheque bearing No.906541 dated 13.04.2004 on ICICI BANK.

Contd...2

ORIGINAL

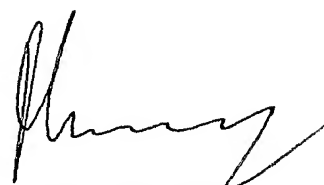
30/CHE/2004

JUN 2004

15 APR 2004

We request that a patent may be granted to us for the said invention.

Dated this 13th day of April, 2004.

A handwritten signature in black ink, appearing to be 'S.D. Ahuja', written in a cursive style.

(S.D. AHUJA)
OF D. P. AHUJA & CO
APPLICANTS' AGENT

To
The Controller of Patents,
The Patent Office,
Chennai

FORM 2

**THE PATENTS ACT, 1970
(39 of 1970)**

**PROVISIONAL SPECIFICATION
(See Section 10)**

TITLE

**REPETITION CODED COMPRESSION FOR ENCRYPTING HIGHLY
CORRELATED DATA**

APPLICANT

**MATRIXVIEW TECHNOLOGIES (INDIA) PRIVATE LIMITED,
of NO. 69, MAHALAKSHMI KOIL STREET, KALAKSHETRA COLONY,
BESANT NAGAR, CHENNAI -600090,
INDIA
AN INDIAN COMPANY**

The following specification particularly describes the nature of the invention

ORIGINAL

33/6/2004

04

Page 1

Technical Field

5

The present invention relates to a method and system of encrypting highly correlated data streams.

Background of the Invention

10

Data compression is of vital importance and has great significance in many practical applications.

15

Security is a significant issue in image compression. Applications such as video-on-demand, pay-per-view and medical imagery require data protection in addition to compression. For example, in a medical imaging application, modern healthcare standards like H17 and DICOM make it compulsory to store patient details for up to five years. It is necessary to compress images to save storage space. Also, it is necessary to ensure that the transmission and storage of these images are secure to maintain the sacrosanct nature of the patient details.

20

Encryption is a secure and trusted method for storing highly sensitive information privately. Encryption is a reversible process by which bits of data are mathematically scrambled and unscrambled using a password key. Encryption transforms the data so that it is unreadable and unintelligible until it is decrypted. Most encryption involves authentication and aims to identify images or documents and their routing through a network. This involves retaining small packages of information in secure form during transmission and remote access.

25

Some encryption techniques include digital watermarking, RSA, Pretty Good Privacy (PGP) and DES. Digital watermarking consists of modifying the original data, and embedding a watermark in the original data. PGP is an open source encryption standard that generates a key pair: a public key and a private key. PGP requires additional transmission of public keys along with the encrypted data. However, this additional transmission results in added data overhead. These prior art encryption techniques involve complex algorithms which require additional computational processing power. Also, these and other encryption techniques involve passwords that may be predictable which make them vulnerable for security to be compromised.

35

Existing open image compression standards are not designed allow the addition of an encryption layer. So when compressed files are encrypted, they do not conform to the open standard and the advantages of using an open standard are not enjoyed.

40

Summary of the Invention

In accordance with a preferred aspect there is provided a method for encrypting highly correlated data wherein each element is compared with a previous element. If they are both equal, a first value is recorded. If they are not both equal, a second value is recorded. The first value may be a 1, and the second value may be a 0. An encryption layer is added to mathematically manipulate the compressed data.

Data compression using RCC is closely related to data encryption. In contrast to data compression where the objective is to reduce the volume of data and achieve reproduction of the original data without any perceived loss in data quality, the objective of data encryption is to transform data into an unreadable and unintelligible form to ensure privacy.

The data may be image data. If image data is encrypted, each element may be a pixel. The first and second values may be stored in a bit plane. A bit plane refers to the memory in a graphic display device which holds a complete one-bit-per-pixel image. Several bit planes may be used in conjunction to give more bits per pixel or to overlay several images or mask one with another. "Bit plane" may sometimes be used as a synonym for "bitmap". For a one-dimensional compression, a single bit plane may be used to store the values. However, for a two-dimensional compression, comparison may be in both horizontal and vertical directions, a separate bit plane being used for each direction.

The bit-planes for the horizontal and vertical directions may be combined by binary addition to form a repetition coded compression bit-plane. Combining may be by binary addition, only the second values being stored for lossless reconstruction of the image. The result of the combining may be repetition coded compression data values. All other image data values may be able to be reconstructed using the repetition coded compression data values, and the bit planes for the horizontal and vertical directions.

Storage in bit planes may be in a matrix. A single mathematical operation may be performed for each element.

In accordance with a further aspect, there is provided an encryption system for encrypting highly correlated data using repetition coded compression, the system comprising a data receiver for receiving digital data; a reshaping block for rearranging the digital data into a matrix of data values; a processor for receiving the matrix of data values and compressing the data values to form compressed data; and a memory for storage of the compressed data, an encryption module for adding an encryption layer to mathematically manipulate the compressed data.

In accordance with another aspect, there is provided a method for encrypting data comprising receiving digital data. The digital data is reshaped into a digital data matrix. Repetitions in the digital data matrix are encoded into a bit-plane index, and stored data values. The compressed data is stored in a storage memory in an encrypted form.

The bit-planes may contain information regarding the repetitions along horizontal and vertical directions. There may be further included the combining of the horizontal and vertical bit-planes by a binary addition operation to give a repetition coded compression bit-plane. There may also be included comparing the repetition coded compression bit-plane with the digital data matrix to obtain final repetition coded compression data values.

The method may further include storing and archiving the repetition coded compression data values along with the horizontal and vertical bit-planes.

The method may be used for an application selected from: medical image archiving, medical image transmission, database system, information technology, entertainment, communications applications, and wireless application, satellite imaging, remote sensing, and military applications.

Both the forward and reverse compression processes of RCC are known only to the developers of the algorithm, ensuring privacy and allowing secure communication of compressed data. ensuring privacy allowing secure communication of compressed data

RCC does not utilise complex modelling and coding models. RCC provides a secure transmission of highly correlated data and images with encryption and decryption on the fly. RCC uses simple, logical transformations and mathematical operations that make the entire algorithm simpler in comparison to the JPEG family of standards and other wavelet transforms.

Advantageously, RCC encryption has been developed to be used without any additional network equipment or application software. This allows compression, encryption and decompression on the fly without any loss of time and increase in storage requirements.

The RCC encryption process offsets any losses due to processing overhead, as it does not require extra time or bits. This allows compression, encryption and decompression on the fly without any loss of time. The RCC encryption system encrypts without reformatting or converting the image, text or data. RCC encryption

- uses bit planes to shift the bits within the bit planes, and even the bit planes themselves can lead to techniques that can simultaneously provide security functions and an overall visual check. Encryption is simultaneous, executed at the same time as the encoding process, thus no added latency affects the speed performance. The RCC algorithm provides inherent encryption for a secure and lossless transmission. RCC encryption may be used together with Adaptive Binary Optimisation (ABO). Alternatively, a third party encryption layer may be added to increase data security.
- When data is encoded and encrypted, a corresponding decryption methodology is generated. This makes each decoder unique to the encrypted data. A Public Key Infrastructure (PKI) approach may be utilised to enable distribution and sharing of encrypted data. The use of security keys such as USB dongles can further be deployed to minimise the issue of piracy and enable data such as music and video to be portable and shared by legitimate consumers.

Applications

- RCC can be used in applications for medical imaging, digital entertainment and document management. Each of these verticals requires RCC to be implemented in a unique way to deliver a robust and powerful end product.

RCC can be deployed in the following forms for commercialisation:

- 1) ASIC or FPGA chips
- 2) DSP or embedded systems
- 3) Standalone hardware boxes
- 4) Licensable software (as DLLs or OCX)
- 5) Software deliverables

Brief Description of the Drawings

- In order that the invention may be fully understood and readily put into practical effect, there shall now be described by way of non-limitative example only a preferred embodiment of the present invention, the description being with reference to the accompanying illustrative drawings in which:

- Figure 1 illustrates the entire image compression system based on repetition coded compression on a hardware implementation;
- Figure 2 is a sample grayscale image of a human brain, which is captured by magnetic resonance imaging ("MRI") to demonstrate the compression able to be achieved by repetition coded compression system;
- Figure 3 is an enlarged image of a small region from Figure 2;
- Figure 4 shows that the image of Figure 2 is made up of many pixels in grayscale;
- Figure 5 shows a 36-pixel region within the sample MRI image of Figure 2;

Figure 6 shows the ASCII value equivalent of the image data values for the image of Figure 2;

Figure 7 shows the application of repetition coded compression along the horizontal direction in the image matrix;

Figure 8 shows the application of repetition coded compression along the vertical direction in the image matrix;

Figure 9 shows the combination of horizontal and vertical bit-planes by a binary addition operation;

Figure 10 shows the total memory required for the 36-pixel region before and after applying repetition coded compression;

Figure 11 shows the application of repetition coded compression to the entire image; and

Figure 12 shows the operational flow for the implementation of repetition coded compression.

Detailed Description of Preferred Embodiments

Certain types of data are highly correlated. For example, image data. This means that the adjacent data values in an image are repetitive in nature. Therefore, it is possible to achieve some compression out of this repetitive property of the image and then apply Huffman coding or other source coding schemes. Such a method would be very efficient.

In repetition coded compression ("RCC"), each element is compared with the previous element. If both of them are equal then a value of "1" is stored in a bit-plane. Otherwise a value of "0" is stored in the bit-plane. Only the difference value is stored in a matrix, instead of storing all the repeating values.

In a one-dimensional performance of the method, only one bit-plane is used to code the repetition in the horizontal direction.

But in a two-dimensional performance of the method, two bit-planes are used to code the repetitions in both the horizontal and the vertical directions. This is more efficient and gives a better compression ratio.

The compression system is based on a mathematical comparison of adjacent image data values. The comparison is performed between adjacent image data values in both the horizontal as well as vertical directions. The bit-planes formed as a result of the comparison in the horizontal and vertical directions are respectively combined by a binary addition method. After this the resultant bit-plane positions are called as RCC bit-planes. The zero values in the RCC bit-plane are stored for lossless reconstruction of the original image. For lossless reconstruction, they are the only values stored. The

stored values correspond to the same locations in the original image matrix as zeros in the RCC bit-plane and are hereinafter called RCC data values. All the other image data values can be reconstructed by using the RCC data values, and the horizontal and vertical bit-planes.

After compression, a software encryption module (not shown) adds an encryption layer to the compressed data, which mathematically manipulates the compressed data.

Figure 1 illustrates the entire image compression system based on repetition coded compression on a hardware implementation. The analog image signals 12 are captured by the camera 10 and are converted into respective digital data 16 by a analog to digital converter 14. This digital data 16 is rearranged into a matrix of image data values by a reshaping block 18. The reshaped image matrix is stored in the embedded chip 20, which performs the entire repetition coded compression system. This therefore gives the compressed repetition coded compression data values 22 and also the bit-planes of data 24 for storage, archival and future retrieval 26.

Figure 2 is a sample image of the human brain which is captured by magnetic resonance imaging (MRI). This sample image may be used to demonstrate the compression achieved by repetition coded compression. It is a grayscale image.

Figure 3 zooms a small region from the sample MRI image of the human brain. This zoomed region may also be used for demonstrating the repetition coded compression system.

Figure 4 shows that the image is made up of lot of pixels in grayscale.

Figure 5 shows a 36-pixel region within the sample MRI image of the human brain.

Figure 6 shows the ASCII value equivalents of the image data values which are originally used for data storage. Each value requires eight bits (1 byte) of data memory. Currently, the 36-pixel region requires about 288 bits or 36 bytes of data memory. After repetition coded compression, this data is compressed and stored with only 112 bits.

Figure 7 shows the application of repetition coded compression along the horizontal direction in the image matrix. This results in the horizontal bit-plane and also the horizontal values stored.

Figure 8 shows the application of repetition coded compression along the vertical direction in the image matrix. This results in the vertical bit-plane, and also the vertical values stored.

Figure 9 shows the combination of horizontal and vertical bit-planes by a binary addition operation. This results in only five zero values which correspond to the final values stored from the original image matrix.

5

Figure 10 shows the total memory required for the 36-pixel region before and after applying repetition coded compression. The original memory requirement was 288 bits. After applying repetition coded compression the memory required is 112 bits.

10 Figure 11 shows the application of repetition coded compression to the entire image. The size is compressed to 44,000 bits from the original 188,000 bits.

Figure 12 shows an implementation of repetition coded compression. The image matrix 1201 is transposed 1202, encoded along the horizontal 1203 and vertical 1204 directions and the respective bit-planes 1205, 1206 are derived. Further compression is achieved by combining the horizontal and vertical bit-planes 1203, 1204 by a binary addition operation. This results in the repetition coded compression bit-plane 1207, which is logically inverted 1208 and compared 1209 with the original image matrix 1201 to obtain the final repetition coded compression data values 1210. The repetition coded compression data values 1210, together with the horizontal and vertical 1206 bit-planes are stored in a data memory 1211 for archival and future retrieval.

The coded data can be further compressed by Huffman coding. This compression of the image data is achieved using the repetition coded compression system. This system is fast as it does not make use of complex transform techniques. The method may be used for any type of image file. In the example given above, the system is applied only for grayscale images. However, it may be applied to color images.

The system of repetition coded compression of images may be applied to fields such as, for example, medical image archiving and transmission, database systems, information technology, entertainment, communications and wireless applications, satellite imaging, remote sensing, military applications.

The preferred embodiment of the present invention is based on a single mathematical operation and requires no multiplication for its implementation. This results in memory efficiency, power efficiency, and speed, in performing the compression. Because of the single mathematical operation involved, the system is reversible and lossless. This may be important for applications which demand zero loss. The compression ratios may be significantly higher than existing lossless compression schemes.

40

Whilst there has been described in the foregoing description a preferred embodiment of the present invention, it will be understood by those skilled in the technology that

many variations or modifications in details of design, constructions or operation may
5 be made without departing from the present invention.

A method for encrypting highly correlated data wherein each element is compared with a previous element and:

- 10 (a) if they are both equal, a first value is recorded;
- (b) if they are not both equal, a second value is recorded; and
- (c) wherein an encryption layer is added.

The data is image data.

15 Each element is a pixel.

The first value is a 1, and the second value is a 0.

The first and second values are stored in a bit plane.

20

A one-dimensional compression, a single bit plane is used to store the values.

For a two-dimensional compression, comparison is in both horizontal and vertical directions, a separate bit plane being used for each direction.

25

The bit-planes for the horizontal and vertical directions are combined by binary addition to form a repetition coded compression bit-plane.

30 The combining is by binary addition, only the second values being stored for lossless reconstruction of the data.

The result of the combining is repetition coded compression data values, all other data values being able to be reconstructed using the repetition coded compression data values, and the bit planes for the horizontal and vertical directions.

35

Storage in bit planes is in a matrix.

A single mathematical operation is performed for each element.

40 An encryption system for encrypting highly correlated data using repetition coded compression, the system comprising:

- (a) a data receiver for receiving digital data;

- (b) a reshaping block for rearranging the digital data into a matrix of data values;
- (c) a processor for receiving the matrix of data values and compressing the data values to form compressed data;
- (d) a memory for storage of the compressed data;
- (e) an encryption module for adding an encryption layer to mathematically manipulate the compressed data.

A method for encrypting data comprising:

- (a) receiving digital data;
- (b) reshaping the digital data into a digital data matrix;
- (c) encoding repetitions in the digital data matrix into a bit-plane index, and stored data values; and
- (d) storing the compressed data in a storage memory in an encrypted form.

The bit-planes containing information regarding the repetitions along horizontal and vertical directions.

The method includes combining the horizontal and vertical bit-planes by a binary addition operation to give a repetition coded compression bit-plane.

The method further includes comparing the repetition coded compression bit-plane with the digital data matrix to obtain final repetition coded compression data values.

The method further includes storing and archiving the repetition coded compression data values along with the horizontal and vertical bit-planes.

The method is used for an application selected from the group consisting of: medical image archiving, medical image transmission, database system, information technology, entertainment, communications applications, and wireless application, satellite imaging, remote sensing applications.

Dated This 13th Day of April 2004

(S.D.AHUJA)

OF D.P.AHUJA&CO
APPLICANT'S AGENT

PROVISIONAL

RCC System for Hardware Implementation

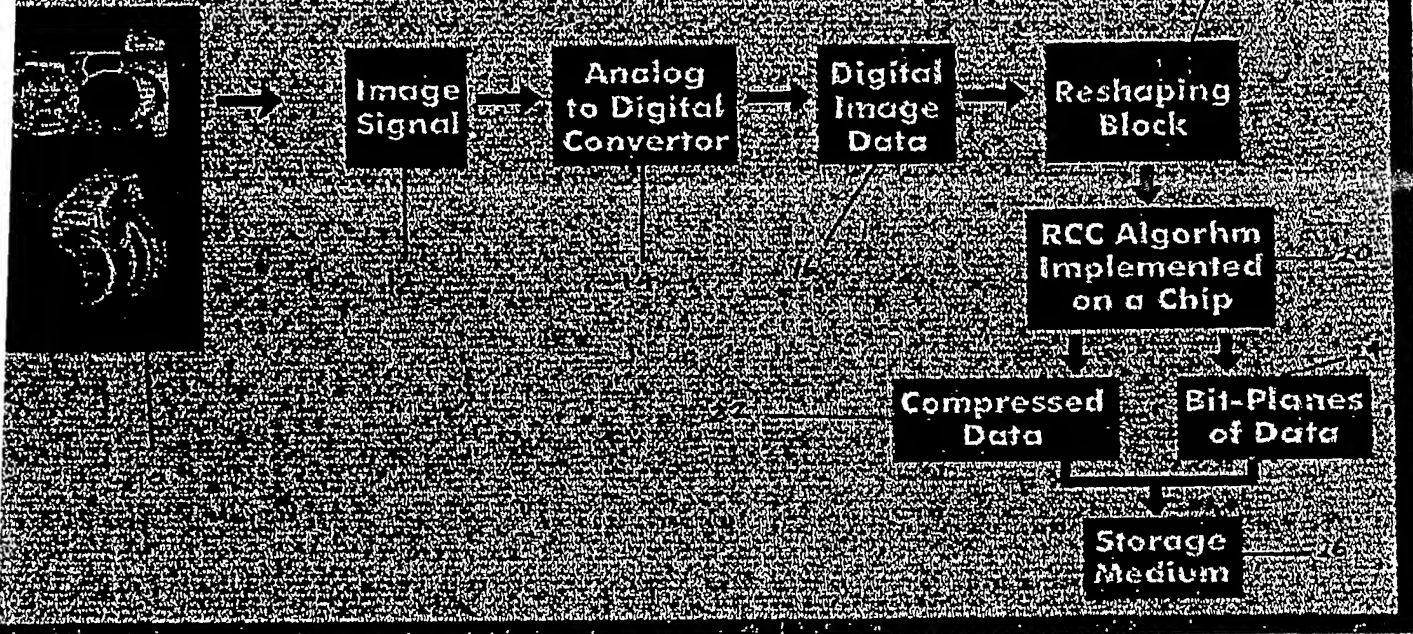


Figure-1

Soumen Mukherjee
(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT

Sample MRI of Human Brain

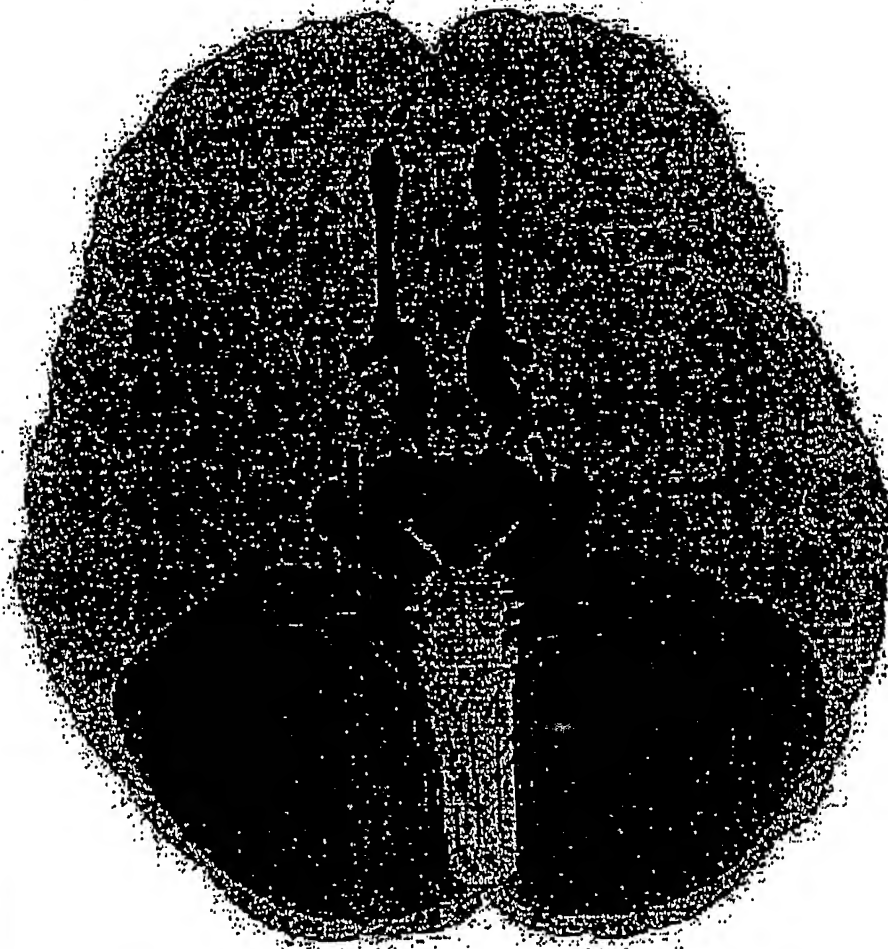


Figure 2

Soumen Mukherjee
(SOUMEN MUKHERJEE)
of D. P. KHUJA & CO.
APPLICANTS' AGENT

IAL

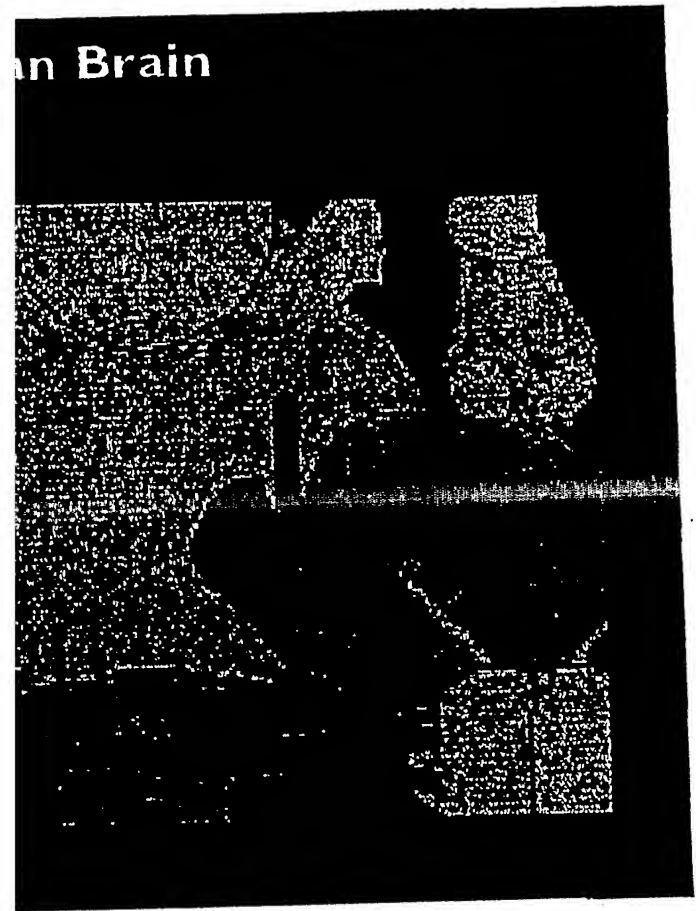


Figure 3

Soumen Mukherjee

(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT

NAL

Brain (Pixel View)

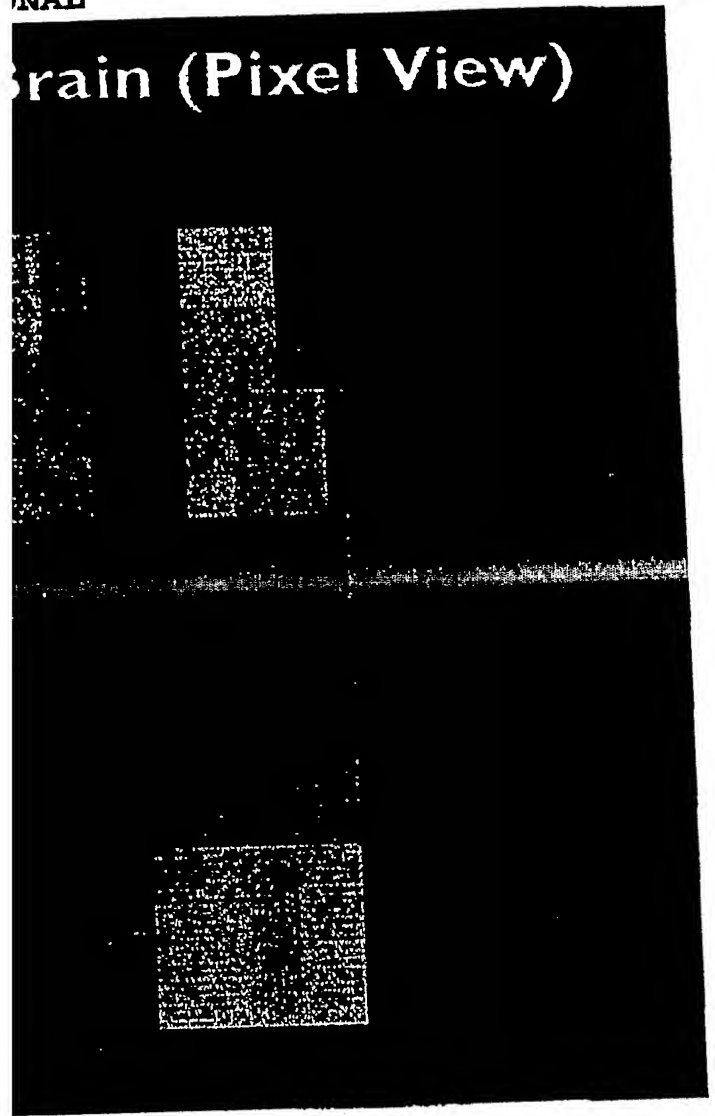


Figure 4

Soumen Mukherjee
(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT

egion



FIGURE 5

Soumen Mukherjee
(SOUMEN MUKHERJEE)
of D. P. *Agarwal & Co.*
APPLICANTS' AGENT

36 Pixel Region

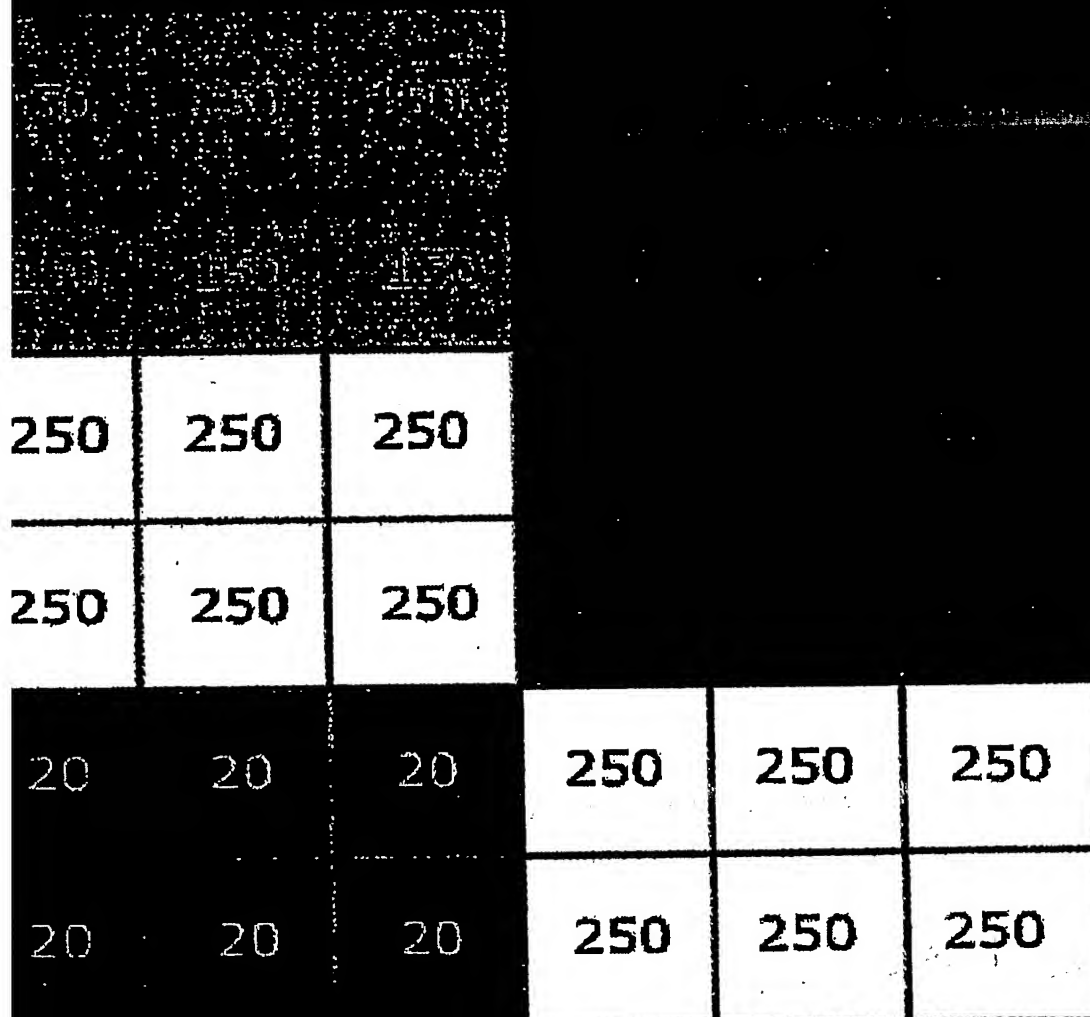


FIGURE 6

Soumen Mukherjee
(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT

ONAL

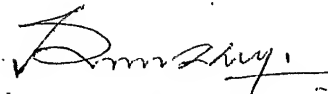
Values Stored

150	100	150	100
250	100	250	100
20	250	20	250

Bit Plane

0	1	1	0	1	1
0	1	1	0	1	1
0	1	1	0	1	1
0	1	1	0	1	1
0	1	1	0	1	1
0	1	1	0	1	1

Figure 7



(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT

Vertical RCC

250	250	250
250	250	250

250	250	250
250	250	250

Rules for adjacent pixels:
 If Same value, bit plane = '1'
 If Different value, bit plane = '0'

Values Stored

150	250	20	150
250	20	150	250
20	100	250	100
250	100	250	

Bit Plane

0	0	0	0	0	0
1	1	1	1	1	1
0	0	0	1	1	1
1	1	1	1	1	1
0	0	0	0	0	0
1	1	1	1	1	1

Figure 8

(Signature)
 (SOUMEN MUKHERJEE)
 of D. P. AHUJA & CO.
 APPLICANTS' AGENT

NO. /CHE/2004

SHEET 9

PROVISIONAL

Bit Plane

	1	1		1	1
0	1	1	0	1	1
	1	1	0	1	1
0	1	1	0	1	1
	1	1		1	1
0	1	1	0	1	1

Bit Plane

	0	0		0	0
1	1	1	1	1	1
	0	0	1	1	1
1	1	1	1	1	1
	0	0			
1	1	1	1	1	1

Final Values Stored

150 100 250
20 250

Figure 9

Soumen Mukherjee
(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT

Original Values

250	150	250
150	100	250
150	100	250

250	250	250
250	250	250

250	250	250
250	250	250

Total Memory Required = 288 bits

Final Values Stored

150 100 250
20 250

After RCC

Total Memory
Required = 112 bits

2008-10-10 Figure 1

(Signature)
(SOUMEN MUKHERJEE
of D. P. AHUJA &
APPLICANTS' AGENT

NO. /CHE/2004

PROVISIONAL

Original Image



Original File Size = 188 kb

File Size After RCC = 44 kb

Figure 11

Soumen Mukherjee
(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT



(SOUMEN MUKHERJEE)
of D. P. AHUJA & CO.
APPLICANTS' AGENT